ДОСЛІДЖЕННЯ МЕТОДІВ ЛОКАЛІЗАЦІЇ ШАХРАЙСЬКИХ ТОЧОК ДОСТУПУ В ЛОКАЛЬНИХ БЕЗДРОТОВИХ МЕРЕЖАХ

Кузнєцов К. А., магістр
Харківський національний університет імені В. Н. Каразіна,
м. Харків, Україна.

Реалізація вимог до виявлення шахрайських точок доступу в локальних бездротових мережах має на увазі поетапний комплекс дій та контрзаходів, які націлені на припинення дій зловмисника та усунення негативних наслідків (таких як, реалізація вірусного коду, захоплення конфіденційної інформації тощо). Це особливо актуальна тема для усіх галузей різного інформаційного та економічного напрямку, бо зараз відбувається великий стрибок в цифровій еволюції. При цьому, з точки зору дотримання вимог інформаційної безпеки в кожному з окремих сегментів виявлення, питання умов локалізації та вибору методу є край важливою задачею. Існує декілька підходів для виявлення шахрайської точки доступу, такі як клієнтський підхід, серверний та гібридний.

Серверний підхід володіє більшою потужністю щодо пам'яті, обчислювальної здатності, що стосується мереж Wi-Fi. Але, як тільки зловмиснику вдасться зламати облікові дані про безпеку, зловмисник зможе легко встановити зловмисну точку доступу або здійснити різні атаки, такі як відмова в службі (DoS) та атака «людина по середині» через зловмисну точку доступу. Будь-яка інсталяція програмного забезпечення або будь-які інші зміни здійснюються в точці доступу, маршрутизаторі, шлюзі або комутаторі. Перевагою такого підходу є те, що клієнту не потрібно турбуватися про встановлення додаткових плагінів або зміни драйвера пристрою, або будь-яких додаткових паролів. В такому способі сервер несе відповідальність за будь-яку точку доступу. Недоліком такого підходу є те, що клієнт не має жодної підказки щодо точки доступу, тобто яка точка доступу є легітимною, а яка зловмисною.

Клієнтський підхід базується на стандарті IEEE 802.11. Даний стандарт зазвичай використовується у смартфонах та ноутбуках. Клієнтський підхід має менше привілеїв та має обмежену обчислювальну потужність, пам'ять, та заряд акумулятора порівняно з сервером. Підхід з боку клієнта — це той підхід, в якому клієнт утримується від підключення до шахрайських точок доступу. Точка доступу також бере участь у цьому підході, наприклад, наявність локальної бази даних сервера DNS (Система доменних імен) тощо.

Та останній підхід — це гібридний. Цей підхід є ефективним, оскільки охоплює нездатність підходу на стороні клієнта та додає потужність підходу на стороні сервера. Необхідно докласти зусиль як з боку клієнта, так і з боку сервера, щоб запобігти виникненню шахрайським точкам доступу. У такому підході і клієнт, і точка доступу беруть активну участь, що знижує ризик

створення несанкціонованої точки доступу або підключення клієнта до точки доступу такого типу. Незважаючи на те, що серверу не вдається запобігти виникненню шахрайської точки доступу, клієнт не зв'яжеться з такою точкою доступу і таким чином, зловмисник не зможе отримати важливі дані з трафіку даних клієнта або запустити будь-які атаки. У цьому підході і клієнт, і сервер наділені повноваженнями.

У підсумку, підхід зі сторони клієнта обмежений порівняно з серверним підходом. Слабкість підходу зі сторони сервера полягає в тому, що коли механізм безпеки виявиться невдалим, клієнт не зможе утриматися від підключення до шахрайської точки доступу. Якщо підходи з стороні клієнта та сервера поєднуються, може бути запропоновано ефективне рішення, яке можна назвати як гібридний підхід, в якому активно беруть участь клієнти та сервери або точки доступу. Отже, навіть якщо сервер не зможе захистити мережу, клієнт не буде підключений до зловмисної точки і, таким чином, буде в безпеці. Кінцева мета — захистити критичні дані клієнта та уникнути різноманітних атак.

Перелік посилань

1. Alotaibi B. Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions / B. Alotaibi, K. Elleithy // Wireless Personal Communications, V. 90, I. 3, 2016. – 33 p. – DOI: 10.1007/s11277-016-3390-x.

2. Sandeep V. Detection of Rogue Access Point Using Various Parameters / V. Sandeep, B. M. P. // S.C. Satapathy et al. (eds.), Proceedings of the International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing 468, – 2017. – pp. 699 - 710. – DOI 10.1007/978-981-10-1675-2_69S.

Анотація

Безпека бездротового зв'язку — справжнє завдання як для мережевих адміністраторів, так і для адміністраторів інформаційної безпеки.

Для виявлення шахрайської точки доступу використовуються різні підходи. Такі підходи можна класифікувати як клієнтський підхід, серверний та гібридний. Кожний метод має свої переваги та недоліки.

Клієнтський має обмежені ресурси і не має надто великого контролю мережі порівняно з серверним. Серед усіх методів гібридний підхід більш ефективний, оскільки мінімізує недоліки методу клієнтської сторони і додає серверне управління для виявлення шахрайських точок доступу. Ця стаття спрямована на вивчення різних методів несанкціонованого доступу до точок доступу.

Ключові слова: шахрайська точка доступу, IEEE 802.11, мережа Wi-Fi.

Аннотация

Защита беспроводной сети — настоящая задача как для сетевых администраторов, так и для администраторов информационной безопасности.

Для выявления мошеннической точки доступа используются разные методы. Такие методы можно классифицировать как клиентский, серверный и гибридный. У каждого метода есть свои преимущества и недостатки.

Клиентский имеет ограниченные ресурсы и не имеет слишком большого контроля сети в сравнении с серверным методом. Среди всех методов гибридный метод более эффективный, поскольку минимизирует недостатки метода с клиентской стороны и добавляет серверное управление для обнаружения мошеннической точки доступа. Эта статься нацелена на изучение разных методов несанкционированного доступа к точкам доступа.

Ключевые слова: мошенническая точка доступа, IEEE 802.11, сеть Wi-Fi.

Abstract

Security of wireless connection is a real task for both the system administrators and information security administrators.

Different approaches are used to find the rogue access point. These approaches can be classified to client approach, server approach and hybrid approach. Each of these ap-proaches have its benefits and drawbacks.

The client approach has limited resources and has not great control of the net in compari-son to the server one. The hybrid one is the most effective among all the approaches due to its minimisation of drawbacks of the client approach and adding server control to re-veal the rogue access point. The goal of this article is to study different methods of un-authorized access to the access points.

Keywords: fraud access point, IEEE 802.11, Wi-Fi net.